REMARKS/ARGUMENTS

These remarks are made in response to the Office Action of June 3, 2004 (Office Action). This response is being filed with a petition for a one month retroactive extension of time with the appropriate fee.

In the Detailed Action, the Examiner has rejected claims 1-40 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,707,889 to Saylor, *et al.* (Saylor) in view of U.S. Patent No. 6,681,327 to Jardin (Jardin).

Prior to addressing the rejections on the art, a brief review of the Applicants' invention is in order. The Applicants' claimed and disclosed subject matter teaches a secure means for conveying VoiceXML content between a network device and a Voice Browser. Specifically, the Voice Browser can authentic itself to the network element. Subsequently, a shared secret can be negotiated between the Voice Browser and the network device. The network device can encrypt VoiceXML content using the shared secret as an encryption key and convey the encrypted content the Voice Browser. The Voice Browser can decrypt the content using the shared secret as a decryption key.

As noted in the background (page 1, line 18 to page 2, line 18), SSL has been typically integrated directly with selected underlying application protocols. Further, SSL compliant **visual** Web Browsers existed at the time of the Applicants' invention. As noted between page 3, lines 16 and page 4, line 21 of the background, at the time of the Applicants' invention, SSL had not been integrated with Voice Browsers. Neither Saylor, Jordin, or combinations thereof provide such teachings or suggestions to integrate SSL with Voice Browsers, as claimed by the Applicants herein.

It should be appreciated that network communications involving Voice Browsers and network devices are unique in that a Voice Browser consumes VoiceXML content received from a network device when presenting that content to a user. The user does not retain a copy of the content that can be visually rendered upon demand, as does a Web user who receives content to be rendered in a visual Web Browser.

Accordingly, Voice XML can be considered an application programming language used to program a voice browser, which programmatically generates audio streams based upon VoiceXML content. In contrast, visual markup language like XML can be considered a presentation language defining a standard file format that can be interpreted by an appropriate visual rendering application. In this respect, XML represents one of a variety of file formats for encoding visual information within an electronic document, much like the ".doc" format, the ".rtf" format, and other electronic document formatting protocols.

Turning now to the rejections on the art, claims 1-40 under 35 U.S.C. § 103(a) as being unpatentable over Saylor in view of Jardin. Saylor discloses a content retrieval system that permits a user of a voice response system (VNAP) to selectively access voice enabled Web pages from a voice server by providing a voice response system with a key (VCode) associated with the desired Web page.

The Examiner cites column 10, lines 17-40 of Saylor as teaching a secured communication referencing "The interpreter passes the request to a voice server which provides **security**, personalization, content retrieval, and billing modules to operate a safe and effective VPage retrieval and delivery system." The **security** is performed by the security component 45 of the voice server 43 illustrated in FIG. 7.

The security 45 component is defined at column 20, lines 33-57 as "authenticating users that dial into the VNAP" and as including a password based authenticating for accessing password secured Web sites. The authenticating of users with the VNAP is further illustrated in FIG. 16, items 1602-1614.

Saylor is silent in regards to a **secured communication session** between the voice server 43 and the voice browser 35. That is, Saylor fails to teach or suggest that the communication channel in which information is conveyed between the voice server and the voice browser should be secured. Consequently, Saylor does not suggest any aspect of the Applicants claimed invention, which includes steps performed to establish a secured communication session (i.e. establish a secure communication channel) between the Voice Browser and the network element. Specifically, Applicants claim the steps of:(from claim 1)

transmitting a request to the network device **to establish a secured communication session** between the Voice Browser and the network device;

authenticating the network device;

subsequent to said authentication, negotiating a shared secret between the network device and the Voice Browser;

encrypting the VoiceXML-based Web content using said shared secret as an encryption key;

exchanging the encrypted VoiceXML-based Web content between the network device and the Voice Browser; and,

decrypting the VoiceXML-based Web content using said shared secret as a decryption key.

Jardin fails to cure the deficiencies of Saylor. Jardin teaches a method and a system for speeding up secure client-server transactions by using a plurality of servers to assure that a server is available to transmit information whenever a client is ready to receive the information. Jardin is silent in regard to performing secured communications between a Voice Browser and a network device and in regard to securely communicating VoiceXML-based Web content.

Referring to claims 7,. 8, 27, and 28, Saylor is cited as teaching that a voice browser and network device are challenged to prove their identities (column 8, lines 10-17; column 17, lines 15-30). Saylor provides no such teaching. Instead, Column 8, lines 10-17 teach that a user profile can store user information such as credit card information. This stored information can be used when needed, instead of prompting a user for the information. Column 17, lines 15-30 permit a user to specify a level of security needed to utilize the stored information, thereby using a stored credit card account to pay for services. As previously noted, Saylor is silent in regards to a **secured communication session** between a network element and a voice browser.

Referring to claims 9 and 10, the Examiner refers to Saylor column 1, lines 51-61, which is not relevant to the Applicants claims. As previously noted, Saylor is silent in regards to a **secured communication session** between a network element and a voice browser.

In summary, neither Saylor, Jardin, nor combinations thereof teach or suggest the Applicants claimed invention since they are silent in regards to establishing a **secured**

communication session between a voice server and a network element. Consequently, the 35 U.S.C. § 103(a) rejections to claims 1-40 should be withdrawn, which action is respectfully requested.

In light of the above, Applicants believe that this application is now in full condition for allowance, which action is respectfully requested. Applicants request that the Examiner call the undersigned if clarification is needed on any matter within this Amendment, or if the Examiner believes a telephone interview would expedite the prosecution of the subject application to completion.

Respectfully submitted,

Date: 10 Sep 2004

Gregory A. Nelson, Registration No. 30,577
Richard A. Hinson, Registration No. 47,652
Brian K. Buchheit, Registration No. 52,667
AKERMAN SENTERFITT
Post Office Box 3188
West Palm Beach, FL 33402-3188
Telephone: (561) 653-5000